UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/877,473	06/08/2001	John M. Davis	211139.90123	9874

26707 7590 11/16/2004

QUARLES & BRADY LLP
RENAISSANCE ONE
TWO NORTH CENTRAL AVENUE
PHOENIX, AZ 85004-2391

EXAMINER	
ELMORE, JOHN E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 11/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/877,473	DAVIS, JOHN M.	
	Examiner	Art Unit	
	John Elmore	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 are examined.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. **Claims 15-18 are rejected under 35 U.S.C. 112, second paragraph**, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "complete set of packets" in claim 15 is a relative term which renders the claim indefinite. The term "complete set of packets " is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. It is uncertain whether "complete set of packets" simply indicates that the hold queue is full or whether it refers to another predetermined number of packets such as the message length. In the interest of compact prosecution, the limitation "complete set of packets" is understood to read "the number of packets that comprise the entire message." Claims 16-18 are rejected by virtue of their dependence on claim 15.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. **Claims 1, 3, 5-8, 10, 12, 13, 21 and 22 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Narad (USPN 6,157,955 – published December 5, 2000) in view of Nortel ("Using the Accelar 710 Server Switch," Nortel Networks, October 11, 1999, as cited in the IDS).

Regarding independent claim 1, Narad discloses an apparatus comprising

a proxy operable to receive a plurality of packets each including an encrypted portion (apparatus receives a stream of packets to be processed, and since processing can include decryption, packets can be received that have been encrypted from the sender; see column 6, line 46, through column 7, line 2),

the proxy operable to buffer the packets until a predetermined number of packets are received (a ring buffer can queue only up to a predetermined number of packets due to memory allocation; see column 7, line 63, through column 8, line 4; column 10, lines 1-3; column 11, line 62, through column 12, line 17; and column 17, lines 29-44),

the proxy further operable to decrypt the encrypted portion of each received packet (column 9, lines 5-9) and forward the decrypted packets to a predetermined destination (TX ring forwards packet to original destination address; column 30, lines 42-43, and column 31, lines 15-25).

But Narad does not explain that the proxy is a proxy that handles traffic in accordance with the Secured Sockets Layer (SSL) protocol.

However, Nortel teaches an SSL proxy (accelerator) used to increase the performance of Web site servers by handling the SSL transactions (page xiii, paragraph 1; page 1-1, paragraph 1; page 2-1, paragraph 2; and page 2-5, paragraph 2) before they reach the Web servers in order to significantly reduce the servers' workload.

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Narad with the teaching of Nortel to provide a cryptographic coprocessor that can encrypt and decrypt packets in accordance with the SSL protocol. One would be motivated to do so in order to handle SSL transactions and thereby significantly reduce the workload of Web servers.

Regarding dependent claim 3, Narad and Nortel further teach an apparatus wherein the encrypted portion of the packets are decrypted when received and the SSL proxy buffers the received packets out of order (encrypted packets placed in decryption queue when received while other packets may be forwarded out-of-order; column 30, lines 42-44 and section 7.2).

Regarding dependent claim 5, Narad and Nortel further teach an apparatus wherein the packets are sent by a client computer and received by a server computer (apparatus receives packet stream from client to server, processes it, and forwards to server; see column 6, lines 42-47; column 113, lines 41-55; and Figure 1).

Regarding dependent claim 6, Narad and Nortel are relied upon for teaching in regard to claims 1 and 5. Narad and Nortel further teach an apparatus wherein the SSL

proxy is operable to receive unencrypted data from the server, encrypt the unencrypted data, and send the encrypted data to a client computer (apparatus receives a stream of packets to be processed, and since processing can include encryption, packets received can be unencrypted; also, the designations of client and server are interchangeable in that the proxy can receive packets from the sender and forward to the other regardless of which computer initiates the session between the two; see column 6, line 42, through column 7, line 6; column 113, lines 41-55; and Figure 1).

Regarding dependent claim 7, and Nortel further teach an apparatus wherein the SSL proxy performs encryption and decryption on packets using a single end-to-end TCP connection between a client computer and a server (apparatus processes packet stream between client and server on same TCP connection and performs encryption and decryption on packets; see column 6, line 42, through column 7, line 6; column 113, lines 41-55; and Figure 1).

Regarding independent claim 8, Narad and Nortel are relied upon for teaching in regard to claim 1, particularly that the apparatus embodies the SSL protocol and that the received packets can contain encrypted payloads.

Narad and Nortel disclose a system for handling SSL traffic comprising:

a client computer operable to initiate an SSL session and to send packets with encrypted payloads (apparatus receives packet stream of encrypted payloads from client to be decrypted; see column 6, lines 42-47; column 113, lines 41-55; and Figure 1).

a server computer operable to support communications with the client computer (server exists apart from apparatus and communicates with client; see column 6, lines 42-47; column 113, lines 41-55; column 7, lines 63-67; and Figure 1); and

a SSL proxy coupling the client computer and the server computer and operable to decrypt the encrypted payloads of each packet and forward the decrypted packets to the server computer (apparatus receives encrypted packet stream from client to server, decrypts it, and forwards to server; see column 6, line 42, through column 7, line 6; column 113, lines 41-55; and Figure 1).

Dependent claim 10 is rejected on the same basis as claim 3 with reliance upon Narad and Nortel for teaching in regard to claim 8.

Regarding dependent claim 12, Narad and Nortel are relied upon for teaching in regard to claim 8. Narad and Nortel further teach an apparatus wherein the SSL proxy is operable encrypt packets sent from the server to the client computer (apparatus receives a stream of packets to be processed, and since processing can include decryption, packets received at proxy can be encrypted from the sender; also, the designations of client and server are interchangeable in that the proxy can receive packets from the sender and forward to the other regardless of which computer initiates the session between the two; see column 6, line 42, through column 7, line 6; column 113, lines 41-55; and Figure 1).

Dependent claim 13 is rejected on the same basis as claim 7 with reliance upon Narad and Nortel for teaching in regard to claim 8.

Regarding independent claim 21, Narad teaches an apparatus for decrypting network data traffic comprising a proxy operable to:

(i) receive packets addressed to a server computer (see rationale for rejection of claim 5), the packets including an encrypted portion, a destination address, and a source address (apparatus supports TCP/IP which contains both a destination and a source address, and the payload can be encrypted; see column 6, line 42, through column 7, line 6; column 90, line 60, through column 91, line 15; column 104, lines 32-39; and Figure 1);

(ii) decrypt the encrypted portions of the received packets (column 6, line 42, through column 7, line 6); and

(iii) send the decrypted portions to a server computer without altering the destination or source address of the received packets (packets are intercepted at the OSI data link layer so the IP addresses remain unmodified when the packets are forwarded; see column 6, lines 46-48; column 7, line 63, through column 8, line 4; column 30, lines 42-44; column 31, lines 15-25; and column 104, lines 33-39).

Dependent claim 22 is rejected on the same basis as the rejection of claims 6 and 21.

4. **Claims 2 and 9 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Narad and Nortel and further in view of Netscape ("Introduction to SSL," Netscape, October 9, 1998).

Regarding dependent claim 2, and Nortel further teach an apparatus that includes a database operable to track information about the packets (column 8, lines 16-19), including what cryptographic "operations to perform" on the packets (Crypto Command Descriptor; see column 16, lines 15-19, and column 27, lines 4-7) and the "encryption context" (column 36, lines 59-65), but Narad does not explicitly explain that this information includes a type of encryption scheme used to encrypt the encrypted portion of the packets.

However, Netscape teaches that the SSL protocol is capable of utilizing a number of alternative encryption types (page 2, last paragraph, and page 3, third paragraph).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Narad and Nortel with the teaching of Netscape to include a database operable to track a type of encryption scheme used to encrypt the encrypted portion of the packets. The particular encryption scheme employed for each packet would be recorded, in the least, in the Crypto Command Descriptor, which describes to the cryptographic coprocessor the operations to perform on each packet. One would be motivated to do so in order to permit the cryptographic coprocessor to handle a variety of encryption schemes in accordance with SSL protocol.

Dependent claim 9 is rejected on the same basis as claim 2 with reliance upon Narad and Nortel for teaching in regard to claim 8.

5. **Claims 4 and 11 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Narad and Nortel and further in view of Bakhtiari et al, hereinafter Bakhtiari, ("A Message Authentication Code based on Latin Squares," Proceedings of Australasian Conference on Information Security and Privacy, 1997).

Regarding dependent claim 4, Narad and Nortel do not explicitly explain a proxy that tracks a message authentication code used to authenticate a message.

However, Bakhtiari teaches that a message authentication code is a common cryptographic tool composed of a checksum and a cryptographic key that is used to authenticate a message and verify that it has not been modified (page 1, first paragraph). Moreover, Narad and Nortel teach the using and tracking of both a checksum (column 36, lines 40, through column 37, line 20) and a cryptographic key (column 27, lines 4-7).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Narad and Nortel with the teaching of Bakhtiari to track a message authentication code used to authenticate a message. One would be motivated to do so in order to facilitate message authentication using a common method.

Dependent claim 11 is rejected on the same basis as claim 4 with reliance upon Narad and Nortel for teaching in regard to claim 8.

6. **Claims 14-18 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Narad and Nortel and further in view of CasheFlow Technical Note, hereinafter CacheFlow, ("SSL Primer," CacheFlow Technical Note, October 2000).

Regarding dependent claim 14, Narad and Nortel are relied upon in regard to the teaching in claim 8. But Narad and Nortel do not explain that the apparatus buffers the packets until a predetermined number of packets arrive, then decrypts the packets and forwards the decrypted packets to the server.

However, CacheFlow teaches an SSL proxy that buffers the packets until a predetermined number of packets arrive, then decrypts the packets and forwards the decrypted packets to the server (proxy buffers the entire message and then decrypts it; see section 3.4.3, particularly step 4).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Narad and Nortel with the teaching of Bakhtiari to track a message authentication code used to authenticate a message. One would be motivated to do so in order to facilitate message authentication using a very common method.

Regarding independent claim 15, Narad and Nortel are relied upon for teaching in regard to claim 1, particularly that the method involves the processing of SSL packets. Narad and Nortel further teach a method comprising:

initializing an SSL session between a client computer and a SSL proxy (apparatus receives packet stream of encrypted payloads from client to be decrypted; see column 6, lines 42-47; column 113, lines 41-55; and Figure 1);

receiving a packet including an encrypted portion at the SSL proxy (since processing can include decryption, packets can be received that have been encrypted from the sender; see column 6, line 46, through column 7, line 2);

determining if the received packet is a SSL packet (PP determines the nature of the packet, and given the teaching of Nortel, can determine whether it is an SSL packet; see column 6, line 56, through column 7, line 6; column 8, lines 8-16; and column 59, lines 51-54);

placing the received packet in a hold queue (arriving packets are queued; see column 7, line 67, through column 8, line 8; and column 30, lines 42-48);

outputting the decrypted packets to a server computer.

But Narad and Nortel do not explicitly explain checking the hold queue for a complete set of packets and decrypting the encrypted portion of each packet once the complete set is received.

However, CacheFlow teaches the conventional SSL proxy method of queuing the stream of arriving SSL packets until a complete set of packets is received at the proxy and then decrypting the encrypted portion of each packet (proxy queues the entire message and then decrypts it; see section 3.4.3, particularly step 4).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Narad and Nortel with the teaching of CacheFlow to queue the stream of arriving SSL packets until the entire message is received at the proxy and then decrypting the encrypted portion of each packet. This could be accomplished in the queuing preceding the PP or by filling the crypto queue

until it holds the entire encrypted message. One would be motivated to do so in order to approximate the conventional SSL proxy method of decrypting the message in its entirety before transmission to the server.

Dependent claim 16 is rejected on the same basis as claim 4 with reliance upon Narad, Nortel, and CacheFlow for teaching in regard to claim 15.

Regarding dependent claim 17, Narad and Nortel further teach that non-SSL packets are sent directly to the server (packets, especially those not requiring cryptographic processing, can be forwarded directly to the destination address; see column 30, lines 42-48, and column 31, lines 14-24).

Regarding dependent claim 18, Narad and Nortel further teach that the step of placing the packets in a hold queue comprises:

placing packets received out of order in a queue (out of order received packets can be queued for processing by the Policy Engine; see column 7, line 63, through column 8, line 4; column 31, lines 1-4; column 109, lines 3-6; and column 111, lines 25-35); and

decrypting packets received in order and forwarding the decrypted packets to a server computer (decryption is performed in order as PE can examine packets by sequence number before making them available to cryptographic coprocessor; see column 8, lines 9-13; column 60, line 50-53; column 61, lines 58-62; column 107, 58-60; column 108, line 24-58; and column 110, lines 58-67);

checking the hold queue to determine if the packet in the queue is next in sequence (column 108, line 63, through column 109, line 6);

releasing the packet from the hold queue if the packet in hold queue is the next in sequence (column 108, line 63, through column 109, line 6; and column 110, lines 58-67); and

getting a new packet if the packet in the hold queue is not the next in sequence (PE can pass packet directly to cryptographic coprocessor by checking sequence number of arriving packets with the next expected sequence number in the queue; see column 31, lines 1-4 and 29-32; column 108, line 24, through column 109, line 6; and column 110, lines 58-67).

Dependent claim 19 is rejected on the same basis as claim 7 with reliance upon Narad, Nortel, and CacheFlow for teaching in regard to claim 15.

Dependent claim 20 is rejected on the same basis as claim 6 with reliance upon Narad, Nortel, and CacheFlow for teaching in regard to claim 15.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Dyer et al, "Application Support Architecture for a High-Performance, Programmable Secure Coprocessor," Proceedings of National Information Systems Security Conference, October 1999. Dyer et al disclose a cryptographic coprocessor that processes a stream of packets at the data link layer.

Smith et al, "Practical Private Information Retrieval with Secure Coprocessors, " IBM RC 21806, July 27, 2000. Smith et al disclose a cryptographic coprocessor that processes a stream of packets at the data link layer.

Holden et al, USPN 5,802,178, published September 1, 1998. Holden et al disclose a cryptographic proxy server.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 703-306-5538. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100